

REMARKS

Claims 1-34 are pending in the present application. Claims 32 and 34 were canceled; and Claims 1-3, 12, 20, 31 and 33 were amended. Reconsideration of the claims is respectfully requested.

I. 35 U.S.C. § 101

The Examiner has rejected Claims 31-34 under 35 U.S.C. § 101 as being directed towards non-statutory subject matter. In response to this rejection, Claims 31 and 33 have respectively been amended to depend from Claim 20, directed to a computer program, and Claims 33 and 34 have been cancelled. Accordingly, Applicants consider that the rejection under 35 U.S. § 101 has been overcome.

II. 35 U.S.C. § 102, Anticipation

The Examiner has rejected Claims 1-7, 10-17, 20-26, and 29-30 under 35 U.S.C. § 102 as being anticipated by U.S. Patent No. 5,966,705 to Koneru et al. The Examiner has also rejected Claim 33 under 35 U.S.C. § 102, as being anticipated by U.S. Patent No. 6,092,196, to Reiche. The rejections under 35 U.S.C. § 102 are respectfully traversed.

In making their invention, as stated in the application at page 5, lines 11-12, Applicants were concerned with communication between a web client and a web site having both secure and non-secure web pages. Applicants recognized that for web sites such as e-commerce web sites, it is necessary to allow for authentication and session management when holding a conversation with a web client. As is well known to those of skill in the art, cookies are a popular method for session management between a web site and a web client. Cookie based session management must incorporate a secure communication protocol, to prevent unauthorized users from stealing sensitive data contained in the cookie. One such protocol is HTTPS (HTTP/SSL).

The above conclusions of Applicants are set forth in the present application, such as at page 1, lines 24-25, page 2, lines 22-23 and page 3, lines 17-19. However, as stated in the application at page 5, lines 1-6, Applicants also recognized that there are significant problems in switching between a secure protocol such as HTTPS and a non-secure protocol such as HTTP, while using a single cookie. For example, switching

BEST AVAILABLE COPY

between HTTPS and HTTP can be troublesome in that when a web client logs on to a web site using HTTPS, a cookie is issued to authenticate the web client. However, if the web client later browses a non-secure page at the web site using HTTP, the same cookie is sent to the web client in clear text. At this point an unauthorized user can steal the cookie. Thus, using a single cookie in this situation, and particularly when a user is continually switching between secure and non-secure web pages, can jeopardize the security of the web site.

Applicants overcome these drawbacks and disadvantages of the prior art by means of the embodiments of the invention, such as the embodiment set forth by Claim 1 of the application. Claim 1 as now amended reads as follows:

1. (Currently Amended) A method of secure session management and authentication between a web site and a web client, said web site having secure and non-secure web pages, said method comprising the steps of:

- a) utilizing a non-secure communication protocol and a session cookie when said web client requests access to said non-secure web pages; and
- b) utilizing a secure communication protocol and an authcode cookie when said web client requests access to said secure web pages, so that utilizations of said authcode cookie are interspersed between utilizations of said session cookie, and at least some utilizations of said session cookie take place after utilizations of said authcode cookie.

From this recitation, Claim 1 clearly teaches that both different cookies and different protocols are used, depending on whether access is requested to non-secure or secure web sites. Applicants consider that Claim 1 as amended distinguishes over the cited Koneru et al. reference, particularly in reciting, in the over-all combination of Claim 1, the following features or limitations:

- (1) Utilizations of the authcode cookie are interspersed between utilizations of the session cookie.
- (2) At least some utilizations of the session cookie take place after utilizations of the authcode cookie.

(3) A non-secure protocol, as well as session cookie, are utilized when accessing a non-secure web site.

The pertinent teaching of the Koneru reference is set forth in the abstract thereof, which reads as follows:

A system and method is disclosed for tracking a user across both secure and non-secure areas on an Internet and/or Intranet site. In one aspect of the system and method, when a user first accesses a non-secure area, such as a public area, the user is assigned a token, such as a globally unique identifier (GUID). The token is used as a key to a database entry on a server computer for tracking the user in non-secure areas. When the user first accesses a secure area, the user is prompted to enter a user identification and a password. The user identification is then used as a key to the database entry, rather than the token. The server then uses the user identification to track the user across both secure and non-secure areas. (Emphasis added.)

This teaching is also emphasized in the Koneru specification, such as at column 6, lines 55-61, wherein it is stated that:

Using the present invention, the method of tracking a user depends upon whether the user has accessed a secure area 78. Prior to accessing a secure area 78, the server 58 tracks the user based upon the GUID stored in the client identifier on the client computer 20. After the user has accessed the secure area 78, the system tracks the user based upon a user identifier entered by the user. (Emphasis added.)

The above teaching of Koneru is further emphasized in Claim 1 thereof, which reads as follows:

1. A method of tracking a user on a client computer as the user accesses secure and non-secure areas on a network server computer, comprising the steps of: upon first accessing a non-secure area, assigning a token representing the user wherein the token does not contain a user identification and using the token as a key for accessing a database entry associated with the user on the server computer; upon first accessing the secure area, receiving a user identifier associated with the user; after accessing the secured area, replacing the token with the user identification as the key to the database entry; and the database entry including customization information associated with user. (Emphasis added.)

From these statements set forth in the Koneru reference, it is abundantly clear that when the user first accesses a non-secure area on a server, the user is assigned a token or a GUID. The token is used as an access key for non-secure areas only until the first time that the user accesses a secure area. Thereupon, the token is replaced with a user identification. From then on, the user identification is used as the access key for both secure and non-secure areas. Thus, after accessing a secure area only one single time, the token associated with non-secure areas is no longer used. This is an essential principle of the Koneru arrangement.

To the extent that there is any equivalency or correspondence between Applicants' Claim 1 and the Koneru disclosure, the session cookie of Claim 1 would correspond to the token or GUID of Koneru, and the authcode cookie of Claim 1 would correspond to the user identification of Koneru. In view of this, it is readily apparent that Koneru not only fails to show or suggest essential features of amended Claim 1, but teaches away from such features, and is totally incompatible therewith.

Applicants' feature (1), referred to above, requires utilizations of the authcode cookie to be interspersed between utilizations of the session cookie. In order for this to occur, one session cookie utilization must take place before utilization of a particular authcode cookie, and another session cookie utilization must take place after the particular authcode cookie utilization. However, the above teaching of Koneru emphasizes that the token thereof, corresponding to Applicants' session cookie, is never used after the first use of the Koneru user identification, which corresponds to Applicants' authcode cookie. Thus, the Koneru arrangement expressly prohibits utilization of the Koneru token from ever taking place, after any utilization of the Koneru user identification.

These teachings of Koneru clearly also are in conflict with the above-referenced feature (2) of Claim 1. Such feature requires that at least some utilizations of the session cookie must take place after utilizations of the authcode cookie.

In regard to the above-referenced feature (3) of Claim 1, pertaining to use of non-secure communication protocol, the Examiner states the following:

As per claims 1, 12 and 20, Koneru discloses . . . (b) a non-secure communication protocol and a session cookie for allowing said web client access to said non-secure web pages (Col 2 lines 12-27); Office Action dated July 14, 2004, page 3.

The above passage of Koneru referred to by the Examiner reads as follows:

To store user information, such as customization information, many sites have a database entry for each user that is accessible using globally unique identifiers ("GUID"). The GUID is a 128-bit string that uniquely identifies each user. The GUID is created by a server when a user first accesses a web site and is stored on the client computer in a small amount of local storage (i.e., local to the client computer) often called a "cookie." When a user returns to the web site, the browser searches local storage to determine if it has a cookie for that web site. If so, the browser transmits the cookie to the server. Typically, however, GUID's are only used to track users in non-secure areas. In secure areas, on the other hand, sites track the user's activity using the user identification (rather than the GUID) that was entered by the user to access the secure area.

Applicants have carefully reviewed this cited passage of the Koneru et al. reference. However, with all due respect to the Examiner, Applicants have been unable to find any reference therein to non-secure communication protocol, or to the utilization thereof when a web client requests access to non-secure web pages, as is recited by Applicants' Claim 1.

Applicants consider that the cited Rieche reference fails, either alone or in any combination with the Koneru et al. reference, to overcome the deficiencies of Koneru discussed above in regard to amended Claim 1.

Claim 2 depends from Claim 1, and is considered to distinguish over the art for the same reasons given in support thereof. In addition, Claim 2 is considered to distinguish over the art, including the Koneru et al. reference, in reciting the step of requesting the session cookie from the web client whenever the web client requests access to the non-secure web pages. As discussed above in connection with Koneru, the Koneru arrangement prohibits use of the token to access non-secure areas, at any time after the first access to a secure area occurs. Thus, Koneru teaches away from requesting

a token or session cookie from the web client at any such time, contrary to amended

Claim 2.

Claim 3 depends from Claims 1 and 2, and is considered to distinguish over the art for the same reasons respectively given in support thereof. In addition, Claim 3 is considered to distinguish over the art, including the Koneru et al. reference, in reciting repeatedly alternating between utilizations of the authcode and utilizations of the session code. In view of the above discussion of Koneru, Applicants consider that neither Koneru nor Reiche, nor any combination thereof, either shows or suggests such feature of amended Claim 3.

Claim 12 is considered to distinguish over the art, including the Koneru et al. reference, particularly in reciting a non-secure communication protocol and a session cookie that is always used for allowing web client access to each one of the non-secure web pages. In view of the above discussion of Koneru, Applicants consider that neither Koneru nor Reiche nor any combination thereof shows or suggests such feature of amended Claim 12. Applicants consider that Claim 12 further distinguishes over Koneru in reciting that the authcode is for allowing web client access only to secure web pages. This clearly contradicts the Koneru teachings.

Independent Claim 20 is considered to distinguish over the art, including both the Koneru et al. and Reiche references, for reasons given in support of Claim 2.

Claims 4-7 and 10-11 respectively depend from Claims 1, 2, and 3, and are each considered to distinguish over the art for the same reasons respectively given in support thereof.

Claims 13-17 respectively depend from independent Claim 12, and are each considered to distinguish over the art for the same reasons given in support thereof.

Claims 21-26, 29-30, and 33 respectively depend from Claim 20, and are each considered to distinguish over the art for the same reasons given in support thereof.

III. 35 U.S.C. § 103, Obviousness

The Examiner has rejected Claims 8-9, 18-19, 27-28, 31-32 and 34 under 35 U.S.C. § 103 as being obvious in view of Koneru et al. combined with Koneru.

Claims 8-9 respectively depend from Claims 1, 2, and 3, and are each considered to distinguish over the art for the same reasons respectively given in support thereof.

Claims 18-19 respectively depend from independent Claim 12, and are each considered to distinguish over the art for the same reasons given in support thereof.

Claims 27-28 and 31 respectively depend from Claim 20, and are each considered to distinguish over the art for the same reasons given in support thereof.

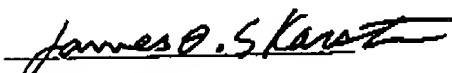
IV. Conclusion

It is respectfully urged that the subject application is patentable over the Koneru et al. and Reiche references and is now in condition for allowance.

The Examiner is invited to call the undersigned at the telephone number listed below if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: October 14, 2004

Respectfully submitted,



James O. Skarsten
Reg. No. 28,346
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 367-2001
Attorney for Applicants

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.